Sonderausgabe 2018/2019

www.mobile-automation.info

SPEZIAL 2018

HANSER

automotive

Mobile Automation

Sensorik/Aktorik

Fahrerassistenzsysteme
Funktionale Sicherheit
Sensoren

Automatisierung/ Steuerung

Automatisierung der Baustelle
Umfeld-Monitoring
V2X-Systeme

Anzeige-/ Bedienelemente

Touch-Displays
HMI

HANSER

AUTOSAR WLAN Kommunikation für Embedded-Systeme

Eine der Herausforderungen der E-Mobility ist die Frage nach neuen Ladekonzepten. Innovative Konzepte setzen dabei zunehmend auf kabelfreie Lösungen, die spezifische Sicherheitsanforderungen und neue Technologien vorrausetzen. Die Firma ServiceXpert verfügt über langjährige Erfahrung in der Automotive Softwareentwicklung, insbesondere für Embedded Steuergeräte mit AUTOSAR.

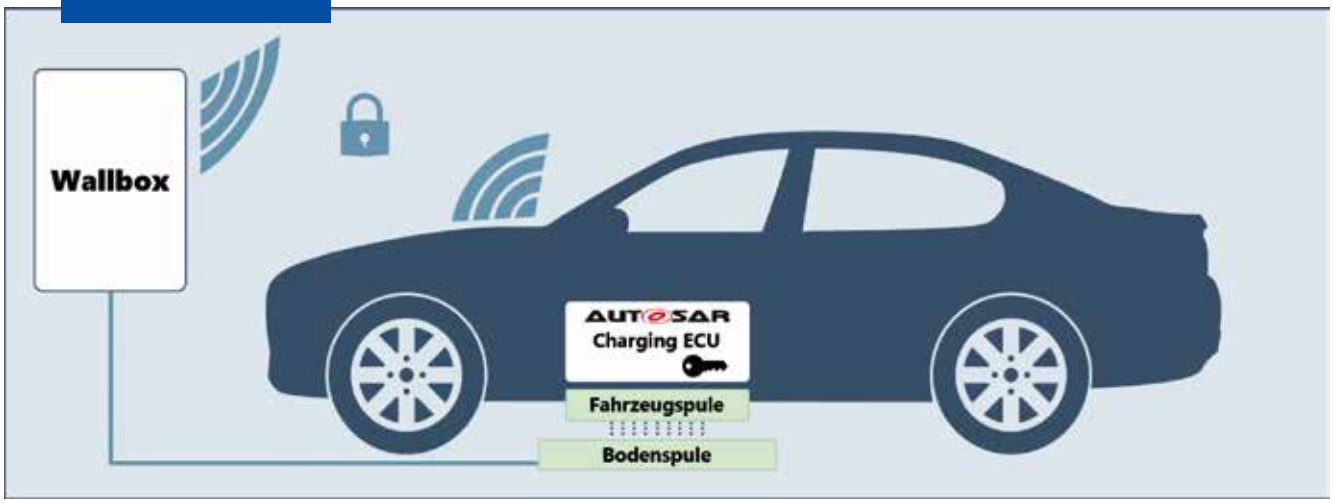
Die zunehmende Elektrifizierung von Fahrzeugen erfordert neue innovative Ladekonzepte. Induktive Lademöglichkeiten bieten weitaus komfortablere Möglichkeiten das Fahrzeug zu laden als herkömmliche kabelgebundene. Hier ist die Kommunikation des Fahrzeugs mit der Ladestation besonders relevant. Heutzutage findet der Datenaustausch über das Ladekabel mittels der sogenannte Powerline Communication Technologie statt. Bei induktiven Systemen ist eine kabellose Kommunikation vor allem in Bezug auf die Benutzerfreundlichkeit wünschenswert.

Ethernet WLAN

Ein etablierter Standard hierfür ist die IEEE-802.11 Norm, besser bekannt als Ethernet WLAN. In Multimediasystemen ist dieser Standard bereits weit verbreitet. In Automotive Steuergeräten ist WLAN ebenfalls eine neue, an Bedeutung gewinnende Technologie.
Auch der sich etablierte Embedded Software Standard AUTOSAR (Classic) spezifiziert und unterstützt die kabellose Kommunikation über WLAN in der neusten Version 4.3.1. Hierzu wird der bereits seit einiger Zeit in AUTOSAR enthaltene Ethernet Stack verwendet, der durch einen Treiber für den gewünschten Ethernet-Transceiver erweitert wird. Der Transceiver bestimmt hierbei die Art der Kommunikation, ob kabelgebunden oder kabellos. Ein Datenaustausch zum Transceiver erfolgt meist über eine SDIO-, RMII- oder SPI-Schnittstelle, welche vom Transceiver Treiber bedient wird. Der Ethernet Stack hingegen ist generisch und unabhängig vom Übertragungsmedium. Teil des Stacks ist das Transmission Control Protocol / Internet Protocol (TCP/IP) Modul, welches sich in drei Scalability Klassen unterteilt. Hierbei kann entschieden werden, ob IPv4, IPv6 oder beide Protokolle unterstützt werden sollen. Basierend auf der Scalability Klasse werden die in der folgenden Tabelle beschriebenen Features unterstützt.

Die Hauptunterschiede zwischen den beiden o. g. Protokollen liegen dabei in der Adressierung der Geräte und

WLAN-Kommunikation beim induktiven Laden.



Bilder: ServiceXpert

Feature	Scalability Klasse 1	Scalability Klasse 2	Scalability Klasse 3
IPv4	✓		✓
ARP	✓		✓
ICMPv4	✓		✓
DHCPv4	✓		✓
Auto-IP	✓		✓
UDP	✓	✓	✓
TCP	✓	✓	✓
IPv6		✓	✓
NDP		✓	✓
ICMPv6		✓	✓
DHCPv6		✓	✓

Das TCP/IP-Modul des Ethernet Stack unterteilt sich in drei Scalability Klassen.

der Zuweisung der Adressen im Netzwerk. IPv6 umfasst einen weit größeren Adressbereich als IPv4, was aufgrund der steigenden Anzahl an Geräten, die mit dem Internet verbunden sind, für die Zukunft Vorteile bietet. Die Adressvergabe wird in IPv4 Netzwerken üblicherweise mittels eines Dynamic Host Configuration Protocol (DHCP) Servers realisiert. Dies ist bei IPv6 nicht mehr nötig, da das Protokoll selber Mechanismen zur Autokonfiguration von IP Adressen vorhält. Zudem unterscheiden sich IPv6 und IPv4 Adressen stark im Aufbau. Eine IPv6 Adresse ist komplexer aufgebaut, beinhaltet aber bereits alle nötigen Informationen über die Netzwerkkonfiguration. Sie setzt sich aus einem Präfix und dem Interface Identifier zusammen. Während bei IPv4 die Unterteilung in Subnetze über Subnetzmasken geschieht, sind diese Informationen bei IPv6 bereits in das Präfix integriert. Die Vergabe des Interface Identifier erfolgt dann in der Regel anhand der MAC Adresse, welche eine gute Basis zur Generierung von einzigartigen Identifiern darstellt.

ISO 15118

Auch im Umfeld induktiver Ladekonzepte betrachtet das ServiceXpert-Team die Tatsache, dass WLAN neue Möglichkeiten für die Funktionalität bei der Fahrzeugkommunikation eröffnet, jedoch sowohl bekannte, als auch neue Sicherheitsrisiken mit sich bringt. Das Kommunikationsprotokoll, die -mechanismen, sowie die Sicherheitsaspekte für das Laden von Elektrofahrzeugen sind in der ISO 15118 spezifiziert. Auch AUTOSAR berücksichtigt bereits den Use-Case des Datenaustausches zwischen Fahrzeug und Ladestation, auch bekannt als Vehicle to Grid (V2G).

Kommunikationsprotokoll

Das in der ISO 15118 definierte Kommunikationsprotokoll ist TCP/IP mit Transport Layer Security (TLS) zur sicheren Datenübertragung. Dabei existieren für TCP/IP bekannte Angriffsszenarien wie z.B. IP Spoofing, SYN Packet Flooding, TCP Session Hijacking usw., die bei einer sicherheitsfokussierten Lösungsentwicklung zu berücksichtigen sind. Auch TLS in der Version 1.2 ist aufgrund der Rückwärtskompatibilität anfällig für Attacken. Ein Angreifer kann sich diese zu Nutze machen, indem er ein Downgrade der Version erzwingt. Verbreitete Angriffstechniken hierbei sind beispielweise DROWN, SLOTH oder POODLE, welche hingegen in der derzeit aktuellsten Version 1.3 von TLS erkannt und abgesichert werden.

Ein weiterer Sicherheitsaspekt der ISO 15118 ist der Authentifizierungsmechanismus basierend auf einer Public Key Infrastructure (PKI) durch den Austausch von Zertifikaten. Dabei wird ein V2G Root-Zertifikat verwendet, um beispielsweise für OEMs oder Ladesäulenbetreiber sogenannt Subordinate Certification Authorities (sub-CA), eigene untergeordnete Zertifikate, zu generieren. Aus den sub-CAs leiten sich anschließend die spezifischen Zertifikate für z. B. Fahrzeuge und Ladesäulen ab.

Die Ablage dieser Daten spielt für die Software eine wichtige Rolle, um einen unbefugten Zugriff von außen zu verhindern. AUTOSAR bietet hierfür einen Crypto Stack, der einen Crypto Service Manager (CSM), ein Crypto Interface (CryIf) sowie Treiber beinhaltet. Die Treiber dienen zur Verschlüsselung der Daten mithilfe von Software- oder Hardwaremechanismen, insofern diese vom Mikrokontroller unterstützt werden.

Fazit

Innovative Technologien wie WLAN Kommunikation mit AUTOSAR und V2G bieten neue spannende Möglichkeiten für die Elektromobilität, bringen jedoch auch komplexe Herausforderungen mit sich. Nicht nur die technische Umsetzung ist dabei von Bedeutung, sondern auch der Aspekt der Sicherheit bei der Datenablage und -übertragung ist elementar.

ServiceXpert nutzt ihr domänenspezifisches Know-how bei sicherheitsrelevanten Lösungen beispielsweise im Umfeld des autonomen Fahrens bei Nutzfahrzeugherstellern und bietet als etablierter Engineering-Partner Softwarelösungen, sowie Beratung für Projekte im Automotive Umfeld. ■

ServiceXpert Gesellschaft für Service-Informationssysteme mbH - A company of the ESG group
www.servicexpert.de

Ergun Yavuz (Bild oben) und **Sören Stein** arbeiten als Systemingenieure, E/E Systemdesign, bei der ServiceXpert GmbH.